Introducción a la Criptografía Moderna

Introducción "Básica" de Teoría de Números, Álgebra Abstracta, Aritmética de Cuerpos Finitos,

"Lo necesario para el curso"

Rodrigo Abarzúa[†],

[†] Universidad de Santiago de Chile
rodrigo.abarzua@usach.cl

April 8, 2014

1. Cuerpos Finitos
   - Grupos
   - Cuerpos
   - Cuerpos primos
   - Extensión del Cuerpos $GF(2^m)$
     - Adición y Sustracción en $GF(2^m)$
     - Multiplicación en $GF(2^m)$
     - Inversión en $GF(2^m)$

Cuerpos Finitos

Antes de dar una definición de los Cuerpos finitos presentaremos algunos conceptos algebraicos básicos.

Grupos

Definición

Un grupo es un conjunto G junto con una operación $*$ en G tal que las siguientes tres propiedades se satisfacen:

- *La operación del grupo $*$ es cerrada, es decir que para cada $a, b \in G$*

$$a * b = c \in G$$

- *La operación $*$ es asociativa, es decir, que para cada $a, b, c \in G$*

$$a * (b * c) = (a * b) * c$$

- *Existe una elemento neutro, que es la identidad (o unidad) denotado por $e \in G$ tal que para todo $a \in G$*

$$a * e = e * a = a$$

- *Para cada $a \in G$, existe un elemento inverso $a^{-1} \in G$ tal que*

$$a * a^{-1} = a^{-1} * a = e$$

Grupos

Definición

Además, si el grupo también satisface

- *Para todo* $a, b \in G$

$$a * b = b * a$$

Entonces el grupo es llamado un grupo abeliano (o conmutativo).

Grupo

Observaciones

- *Es fácil demostrar que el elemento identidad* $\mathbf{e}$ *y el inverso* a^{-1} *de un elemento* $a \in G$ *es único.*
- *Por otro lado,* $(a * b)^{-1} = b^{-1} * a^{-1}$ *para todo* $a, b \in G$*.*
- *Se debe hacer notar que la operación* $*$ *es solo una notación para diferenciarse de la multiplicación corriente.*
- *Cuando se trabaje con grupos se debe dejar claro cual es la operación del grupo.*

Grupo

La ley asociativa nos garantiza que la expresión

$$a_1 a_2 a_3 \cdots a_n \quad \text{con} \quad a_j \in G \text{ para } 1 \leq j \leq n \ .$$

no es ambiguo, desde que no es necesario insertar paréntesis, la expresión siempre representa el mismo elemento en G.

Para indicar la composición n-veces $a \in G$ consigo mismo, donde $n \in \mathbb{N}$, se escribirá:

$$a^n = aa \cdots a, \qquad n \text{ factores de } a.$$

si utilizamos la notación multiplicativa del grupo, denotaremos a^n como las n potencias de a.

Si usamos la notación aditiva para la operación $*$ en G, escribiremos

$$na = a + a + \cdots + a \qquad n \text{ sumandos de } a.$$

Grupo

Ejemplo

- *Sea G en conjunto de los números enteros con la operación de la adición.*
- *El conjunto G de los restos de todos los enteros de la división por 7 es decir,*

$$G = \{[0], [1], [2], [3], [4], [5], [6]\}.$$

la operación del grupo de adición de a y b en G es el resto al dividir la suma de $a + b$ por 6.

Grupo

Definición

Un grupo multiplicativo G se dice cíclico si existe un elemento $a \in G$ tal que para cualquier elemento $b \in G$ existe algún entero j con $b = a^j$. Tal elemento a es llamado un generador de un grupo cíclico, y se denota por $G =< a >$.

Observaciones

- *Es fácil ver todo grupo cíclico es conmutativo.*
- *Además el generador de una grupo no necesariamente es único, por ejemplo $\mathbb{Z}$ posee como generadores el 1 y el -1.*

Definición

Un grupo se dice finito si contiene un número finito de elementos. El número de elementos en un grupo finito se llama el orden. Denotaremos $|G|$ para el orden de un grupo finito.

Cuerpos

La estructura algebraica en la cual tenemos las cuatro operaciones, es decir, *addición, subtracción, multiplicación y división*. Es la estructura algebraica conocida como Cuerpo.

Cuerpos

Definición

Un cuerpo F es un conjunto de elementos con las siguientes propiedades:

- *Todos los elementos de F forman un grupo aditivo con la operación del $+$ y su elemento neutro 0.*
- *Todos los elementos de $F - \{0\}$ forman un grupo multiplicativo con la operación del grupo $*$ y elemento neutro 1.*
- *Se cumple la ley distributiva, es decir, para todo $a, b, c \in F$*

$$a(b + c) = (ab) + (ac).$$

Ejemplo

Algunos cuerpos:

- *El conjunto de los números reales $\mathbb{R}$ es un cuerpo.*

Cuerpos

Teorema

Un cuerpo de orden m sólo existe si m es una potencia de un número primo, es decir $m = p^n$ para algún entero positivo n y algún entero primo p. El primo p es llamado la característica del cuerpo finito.

Cuerpos Primos

Observación

Los elementos de un cuerpo finito denotado por $GF(p)$ puede ser representado por los enteros $0, 1, \ldots p-1$. Las dos operaciones del cuerpo son la adición entera modular y la multiplicación entera modular (todo esto modulo p.)

Teorema

Sea p un número primo. El anillo de enteros $\mathbb{Z}_p$ denotado por $GF(p)$ que se dice un cuerpo primo, o un cuerpo de Galois con un número primo de elementos. Todos los elementos no nulos de $GF(p)$ tienen inverso. La aritmética en $GF(p)$ se realiza modulo p.

Ejemplo

Consideremos el cuerpo finito $GF(5) = \{0, 1, 2, 3, 4\}$ *las siguientes tablas describen como sumar y multiplicar dos elementos*

$+$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	5	1
3	3	4	5	0	2
4	4	5	0	1	3

Observar que los inversos aditivos son: $-0 = 0$, $-1 = 4$, $-2 = 3$, $-3 = 2$, $-4 = 1$

$*$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Observar que los inversos multiplicativos son: 0^{-1} *no existe,* $1^{-1} = 1$, $2^{-1} = 3$, $3^{-1} = 2$, $4^{-1} = 4$.

Un importante ejemplo de cuerpos primos es $GF(2)$, que es el cuerpos finito mas pequeño que existe.

Ejemplo

Consideremos el cuerpo finito $GF(2) = \{0, 1\}$. *La aritmética del cuerpo es:*

Adición		
$+$	0	1
0	0	1
1	1	0

Multiplicación		
$*$	0	1
0	0	0
1	0	1

Extensión del Cuerpos $GF(2^m)$

Observaciones

- *Observemos que* 2^m *no es un número primo, entonces las operaciones de la adición y la multiplicación no se pueden representar por números enteros modulo* 2^8. *Tales cuerpos con* $m > 1$ *son llamados extensión de cuerpos o "extension fields".*
- *Los elementos de estos cuerpos son representados por polinomios y la aritmética de cuerpos que se realiza es la aritmética de polinomios.*
- *En una extensión de cuerpos* $GF(2^m)$ *no se representan por enteros sino por polinomios con grado máximo de* $m-1$ *y los coeficientes de estos polinomios están en* $GF(2)$.

Extensión del Cuerpos $GF(2^m)$

Ejemplo

El cuerpo que utilizamos en el algoritmos AES, es el $GF(2^8)$, *entonces cada elemento* $A \in GF(2^8)$ *es representado por el polinomio:*

$$A(x) = a_7 x^7 + \cdots + a_1 x + a_0, \quad a_i \in GF(2) = \{0, 1\}.$$

- *Observar que hay* $2^8 = 256$ *polinomios. Es decir que* $GF(2^8)$ *tiene* 256 *polinomios.*
- *También se debe observar que cada polinomio se puede almacenar de la forma vectorial de* $8-$*bits, solo almacenando los coeficientes de* $A(x)$

$$A = (a_7, a_6, a_5, a_4, a_3, a_2, a_1, a_0)$$

Adición y Sustracción en $GF(2^m)$

Dados $A(x) = a_{m-1}x^{m-1} + \cdots + a_0$ y $B(x) = b_{m-1}x^{m-1} + \cdots + b_0 \in GF(2^m)$. La adición se define como:

$$C(x) = A(x) + B(x) = \sum_{i=0}^{m-1} c_i x^i, \quad c_i \equiv a_i + b_i \bmod 2$$

y la diferencia se calcula como:

$$C(x) = A(x) - B(x) = \sum_{i=0}^{m-1} c_i x^i, \quad c_i \equiv a_i - b_i \bmod 2$$

Ejemplo

Dado $A(x) = x^7 + x^6 + x^4 + 1$ *y* $B(x) = x^4 + x^2 + 1$ *entonces* $C(x) = x^7 + x^6 + x^2$

Multiplicación en $GF(2^m)$

Dados $A(x)$ y $B(x) \in GF(2^m)$. La adición se define como:

$$A(x) \cdot B(x) = (a_{m-1}x^{m-1} + \cdots + a_0) \cdot (b_{m-1}x^{m-1} + \cdots + b_0)$$
$$C^{'}(x) = c^{'}_{2m-2}x^{2m-2} + \cdots + c^{'}_0,$$

Donde:

$$c^{'}_0 = a_0 b_0 \bmod 2$$
$$c^{'}_1 = a_0 b_1 + a_1 b_0 \bmod 2$$
$$\vdots$$
$$c^{'}_{2m-2} = a_{m-1} b_{m-1} \bmod 2$$

El polinomio $C(x)$ que se considera para la operación de la multiplicación de $A(x) \cdot B(x)$ sera el resto al dividirlo por un polinomio irreductible $P(x)$ que caracteriza al cuerpo $GF(2^m)$. Para comprender este polinomio $P(x)$ presentaremos los siguientes teoremas de cuerpos finitos.

Teorema

Sea F un cuerpo y f un polinomio mónico de grado positivo n sobre F. Entonces el $F[x]/(f)$ es un cuerpo si y solo si f es un polinomio irreducible.

Ejemplo

$$F = \mathbb{R}[x]/(x^2+1) = \{r_0 + r_1\alpha : r_0, r_1 \in \mathbb{R} y \alpha^2 + 1 = 0\}$$

Sea p un número primo y $q = p^n$. entonces el cuerpo de orden q (es decir, que posee q elementos) y denotado por $GF(q)$ o $\mathbb{F}_q$

Teorema

Sea $q = p^n$. Si f es un polinomio irreductible sobre $GF(p)$ de grado n entonces $GF(q) \cong GF(p)[x]/(f)$

Ejemplo

Se puede ver que $f(x) = x^2 + x + 1$ *tiene grado* 2 *y no posee raíces en* $GF(2)$*, luego es un polinomio irreducible en* $GF(2)$*. Entonces el* $GF(2^2)$ *se puede ver como* $GF(2)[x]/(f)$ *(formalmente se dicen isomorfos). Los elementos de* $GF(4)$ *se representan por polinomios* $0, 1, x, x+1$*. Por ejemplo la multiplicación de* x *por* $x+1$ *es:* $x(x+1) = x^2 + x \equiv 1 (\mathrm{mod}\, f)$*. En las siguientes tablas presentamos la adición y la multiplicación en* $GF(4)$

Adición en $GF(2^2)$

$+$	0	1	x	$x+1$
0	0	1	x	$x+1$
1	1	0	$x+1$	x
x	x	$x+1$	0	1
$x+1$	$x+1$	x	1	0

Multiplicación en $GF(2^2)$

$\cdot$	0	1	x	$x+1$
0	0	0	0	0
1	0	1	x	$x+1$
x	0	x	$x+1$	1
$x+1$	0	$x+1$	1	x

Ejemplo

Ejemplo

Considere el cuerpo finito $GF(2^3)$ *visto (via isomorfismos)* $\mathbb{F}_2[x]/(x^3+x+1)$. *El polinomio* x^3+x+1 *es irreducible en* $GF(2)$ *ya que tiene grado 3 y no tiene raices en* $GF(2)$.

Adición en $GF(2^3)$

$+$	0	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
0	0	1	x	$x+1$	x^2	x^2+1		
1	1	0	$x+1$	x	x^2+1	x^2		
x	x	$x+1$	0	1	x^2+x	x^2+x+1		
$x+1$	$x+1$	x	1	0	x^2+x+1	x^2+x		
x^2	x^2	x^2+1	x^2+x	x^2+x+1	0	1		
x^2+1	x^2+1	x^2	x^2+x+1	x^2+x	1	0		
x^2+x	x^2+x	x^2+x+1	x^2	x^2+1	x	$x+1$		
x^2+x+1	x^2+x+1	x^2+x	x^2+1	x^2	$x+1$	x		

Ejemplo

Ejemplo

Considere el cuerpo finito $GF(2^3)$ *visto (via isomorfismos)* $\mathbb{F}_2[x]/(x^3+x+1)$. *El polinomio* x^3+x+1 *es irreducible en* $GF(2)$ *ya que tiene grado 3 y no tiene raices en* $GF(2)$.

Multiplicación en $GF(2^3)$

$+$	0	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
0	0	0	0	0	0	0		
1	0	1	x	$x+1$	x^2	x^2+1		
x	0	x	x^2	x^2+x	$x+1$	1		
$x+1$	0	$x+1$	x^2+x	x^2+1	x^2+x+1	x^2		
x^2	0	x^2	$x+1$	x^2+x+1	x^2+x	x		
x^2+1	0	x^2+1	1	x^2	x	x^2+x+1		
x^2+x	0	x^2+x	x^2+x+1	1	x^2+1	$x+1$		
x^2+x+1	0	x^2+x+1	x^2+1	x	1	x^2+x		

Entonces la definición de la operación del producto es:

Definición

Sea $A(x), B(x) \in GF(2^m)$, *se*

$$P(x) = \sum_{i=0}^{m} p_i x^i, \text{ dondep}_i \in GF(2)$$

un polinomio irreduccible. La multiplicación de dos elementos $A(x), B(x)$ *se calcula:*

$$C(x) \equiv A(x) \cdot B(x) \bmod P(x)$$

entonces para definir el $GF(2^m)$ requiere un polinomios irreducible $P(x)$ de grado m con coeficientes en $GF(2)$. Se debe observar que no todo polinomio es irreducible. Por ejemplo el polinomio

$$x^4 + x^3 + x + 1 = (x^2 + x + 1)(x^2 + 1)$$

luego este polinomio no puede definir el cuerpo $GF(2^2)$

Ejercicios

Dado el cuerpo $GF(2^4)$ *cuyo polinomio irreducible que lo caracteriza es* $P(x) = x^4 + x + 1$, *entonces multiplicar los polinomios* $A(x) = x^3 + x^2 + 1$ *y* $B(x) = x^2 + x$

Inversión en $GF(2^m)$

Dado un cuerpo finito $GF(2^m)$ y si correspondiente polinomio irreducible $P(x)$ el inverso $A^{-1}(x)$ de un elemento $A(x) \in GF(2^m)$ se define como:

$$A^{-1}(x) \cdot A(x) = 1 \bmod P(x)$$

Ejemplo

Anteriormente vimos en el ejemplo, $f(x) = x^2 + x + 1$ tiene grado 2 y no posee raíces en $GF(2)$, luego es un polinomio irreducible en $GF(2)$. Entonces el $GF(2^2)$ se puede ver como $GF(2)[x]/(f)$ (formalmente se dicen isomorfos). En las siguientes tablas presentamos la multiplicación en $GF(4)$

Multiplicación en $GF(2^2)$

$\cdot$	0	1	x	$x+1$
0	0	0	0	0
1	0	1	x	$x+1$
x	0	x	$x+1$	1
$x+1$	0	$x+1$	1	x

Inversión en $GF(2^m)$

Ejemplo

Entonces por ejemplo el inverso de $x+1$ *es el polinomio* x *ya que: Se observa en la tabla que:*

$$(x+1)\cdot x = x^2 + x \equiv 1 \bmod f(x)$$